CITY OF MADISON, WISCONSIN

AN ORDINANCE

Creating Section 23.61 of the Madison General Ordinances to establish Surveillance Technology guidelines for Departments.

PRESENTED
REFERRED President's Work Group to Develop City-Wide Surveillance Equipment & Data Management Policies

Drafted by: Marci Paulsen

Date: August 26, 2019

SPONSORS: Alder Kemble, Alder Baldeh, Alder Carter

DRAFTER'S ANALYSIS: This ordinance requires all Departments to provide notification to the Mayor and Common Council before obtaining or using surveillance technology. The ordinance requires all Departments to provide an annual report on its use of surveillance technology to the Common Council and public. The ordinance creates several exceptions for the approval process outlined within the ordinance, including when there is an emergency or when the surveillance technology involves information that must remain confidential. This ordinance establishes several definitions including surveillance data and surveillance technology.

****

The Common Council of the City of Madison do hereby ordain as follows:

1. Section 23.61 entitled "Use of Surveillance Technology" of the Madison General Ordinances is created to read as follows:

"**23.61 USE OF SURVEILLANCE TECHNOLOGY.**

(1) Intent and Purpose. City of Madison Departments have identified a wide variety of legitimate business reasons to use surveillance technology. The Common Council recognizes the need to carefully balance the need for surveillance for gathering data, public safety and the prosecution of crimes with the public's right to privacy and protection from unreasonable searches and protection of civil liberties, including freedom of speech or association. The Common Council desires to adopt a citywide surveillance technology and surveillance data management policy that is consistent for all City Departments and covers all type of surveillance equipment usage and surveillance data management.

(2) Definitions.

"City-wide Network" means the City's IT infrastructure which is connected using high speed fiber optic connections which allows City employees to share communications, software, hardware devices, and data and information..

"Information Technology Director" means the head of the City Information Technology Department.

"Department" means any agency, department, or division of the City.

"Sensitive Surveillance Technology Information" means any information about Surveillance Technology ~~that~~ of which public disclosure ~~of~~ would unreasonably expose or endanger City infrastructure; would adversely impact operations of City agencies; or may not be legally disclosed.

"Surveillance" means observation of a place, person, group, or ongoing activity in order to gather information.

Commented [KK1]: Per Ledell Zellers

Approved as to form:

Michael P. May, City Attorney

"Surveillance data" means any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.

"Surveillance technology" means any hardware, software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or other personally identifiable information of members of the public for the purpose of surveillance. Surveillance technology includes but is not limited to the following: cell site simulators; automatic license plate readers; gunshot detection systems; facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed; and unmanned aircraft systems equipped with remote video capabilities. Surveillance technology does not include the following devices:

1. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are widespread in use by the City;
2. Audio/video teleconference systems;
3. City databases and enterprise systems that contain information, including, but not limited to, human resource, permit, license and business records;
4. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;
5. Information technology security systems, including firewalls and other cybersecurity systems;
6. Systems or databases that capture information where an individual knowingly and voluntarily consented to provide the information, such as applying for a permit, license or reporting an issue;
7. Physical access control systems, employee identification management systems, and other physical control systems;
8. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, or water or sewer functions;
9. Manually-operated technological devices used primarily for internal City and Department communications and are not designed to surreptitiously collect surveillance data, such as radios, cell phones, personal communications devices and email systems;
10. Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designated to be used surreptitiously and whose function is limited to manually capturing and manually downloading video and/or audio recordings;
11. Devices that cannot record or transmit audio or video or electronic data or be remotely accessed, such as vision-stabilizing binoculars or night vision goggles;
12. Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
13. Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the course of providing City services;
14. Parking Ticket Devices;
15. Equipment used on a temporary basis for investigations and in accordance with City policies;
16. Cameras intended to record activities at City facilities in nonpublic areas;
17. Police Department interview rooms, holding cells, and Police Department internal security audio/video recording systems; and
18. Police Department records/case management systems, Live Scan, Computer Aided Dispatch (CAD).

(3) Applicability. This ordinance applies to all Departments that do any of the following:

(a) Currently uses or has access to any surveillance technology

Commented [KK2]: Ledell Zellers: "What is an example of this?"

Commented [KK3]: Ledell Zellers: "What is "Live Scan"?"

Commented [KK4]: Per Ledell Zellers

(b) Seeks funds for new surveillance technology including applying or accepting grants, state or federal funds or other donations;

(c~~b~~) Acquires new surveillance technology, with or without a cost~~;~~ or

(d)~~(c)~~ E~~e~~nters into a contract~~n agreement~~ with any other entity to share surveillance technology or surveillance data~~; and~~ ~~.~~

(e) All city agencies shall abide by section 5, Reporting Process, to submit annual reports on all new and existing agency surveillance technology.

(4) Approval Process. As of January 1, 2020, all Departments must comply with this subsection prior to any use of new surveillance technology.

(a) All Department requests to purchase, acquire or contract for the use of new Surveillance Technology that will connect to the City-wide Network ~~enterprise system~~ will be referred to the Common Council via the budget process or through a resolution. The resolution will include the information specified in APM 3-17 related to the approval process for surveillance technology, as applicable. The Department's request for Surveillance Technology will be approved only upon the determination that the benefits to the citizens and residents of the City outweigh the costs; that the proposal will not endanger civil liberties and civil rights and that, in the judgment of the Common Council, no alternative with a lesser economic cost or impact upon civil rights or civil liberties would be as effective.

(b) All Departments will notify the Information Technology Director, the Mayor and Common Council leadership of any request to purchase, acquire or contract for the use of new Surveillance Technology that is not connected to the ~~C~~City-wide Network ~~enterprise system~~. The Department will post on the Department's website notice to the public of its intent to obtain or use new surveillance technology ~~to the public on the Department's website~~. The Department will provide further notification to the public as outlined in APM 3-17.

(c) All Departments must comply with the procedure outlined in APM 3-17 when moving or adding cameras on the citywide enterprise camera system.

~~(c) A Department does not need to comply with the above subdivisions if the information involves Sensitive Surveillance Technology Information and the Department provides the basis for exemption to the Information Technology Director. The Information Technology Director will notify the Mayor and Common Council Leadership of the exemption.~~

(5) Reporting Process.

(a) Each Department will conduct an annual review of its Surveillance Technology and ~~insure~~ ensure compliance with this section.

(b) Each Department will complete an Annual Surveillance Technology Report which will be submitted to the Common Council. The Annual Surveillance Technology Report will include:

1. An inventory of current Surveillance Technology and the applicable policies;
2. How the Department has used the data collected by its Surveillance Technology;
3. How any Surveillance Data is being shared with other entities;
4. How well Surveillance Data management protocols are safeguarding individual information; and
5 Whether the Department has received any complaints or concerns about its Surveillance Technology use and the resolution of said complaints.

(c) The Common Council shall review and take action on the resolution accompanying the Annual Surveillance Technology Report.

(6) Exceptions. This ordinance does not apply to the following:

(a) ~~Federal Property Disposition Programs.~~ If the Surveillance Technology is available through federal property disposition programs and/or the purchase or acquisition decision must be executed quickly, such acquisition may be made. However, if the Surveillance Technology is obtained under this subdivision, the Department must apply for approval as described in subsection (4) within fourteen (14) days and before installation or use of said equipment. ~~If approval is denied the Surveillance Technology shall be returned within sixty (60) days after approval was denied.~~

(b) Emergency Situations. In the event of an emergency, that poses an imminent and serious risk of death or substantial bodily harm, a Department may acquire

Commented [KK5]: Possible addition per last week meeting: change in use for a purpose substantially different than originally approved.

Commented [KK6]: Ledell Zellers: "Unclear what information must be included in resolution."

Commented [KK7]: Ledell Zellers: "If we are saying that the surveillance must "not endanger civil liberties and civil rights", how can an alternative have a "lesser…impact upon civil rights or civil liberties"? "

Commented [KK8]: Per Ledell Zellers: "As far as I can tell the only significant "further notification to the public" which is outlined in APM 3-17 is the potential of holding a public meeting…and the statement "If the mayor and Common Council leadership request that a Department notify residents…" which conflicts with the ordinance since the ordinance requires notification of residents on the Dept website."

Commented [KK9]: Per Ledell Zellers

Commented [KK10]: Ledell Zellers: "What resolution? Where does it require a resolution to accompany the Annual Surveillance Technology Report?"

Surveillance Technology without prior Common Council approval, for the sole purpose of preventing or mitigating such risk, if the Department reasonably believes the acquisition of such Surveillance Technology will result in reduction of said risk. The Department's use of the Surveillance Technology must cease when such risk no longer exists or the use of the Surveillance Technology can no longer reasonably reduce the risk. The Department shall apply for approval of the Surveillance Technology per subsection (4) of this ordinance within fourteen (14) days of cessation of the risk that prompted purchase of said technology. The use of the Surveillance Technology must be documented in the Department's Annual Surveillance Technology Report.

(c) Technical Patch or Upgrade. A Department, in consultation with the City Information Technology Department without approval, may apply a technical patch or upgrade that is necessary to mitigate threats to the City's infrastructure, even if the patch or upgrade materially alters the surveillance capabilities of the technology. However, such patch or upgrade, if it does materially alter the surveillance capability of the technology, must be highlighted in the Annual Surveillance Technology Report.

(d) Sensitive Surveillance Technology Information. Sensitive Surveillance Technology Information is exempt from the requirements in the Ordinance. Departments will provide the basis for exemption to the Information Technology Director. The Information Technology Director will notify the Mayor and Common Council Leadership of the exemption.